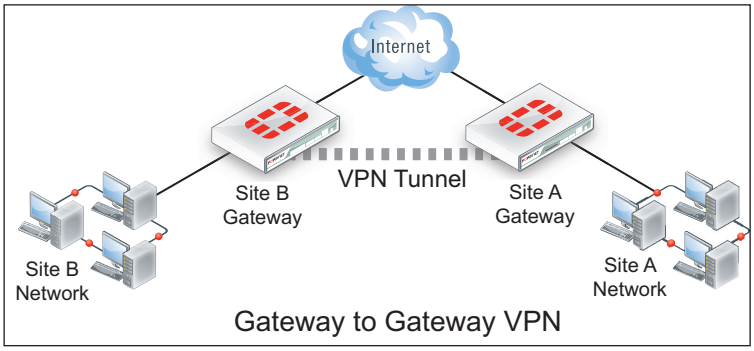
Virtual Private Networks (VPNs)

FortiOS supports IPsec and SSL VPNs that are compatible with industry standards, providing a high level of flexibility, and are accelerated by FortiASIC hardware.

Overview

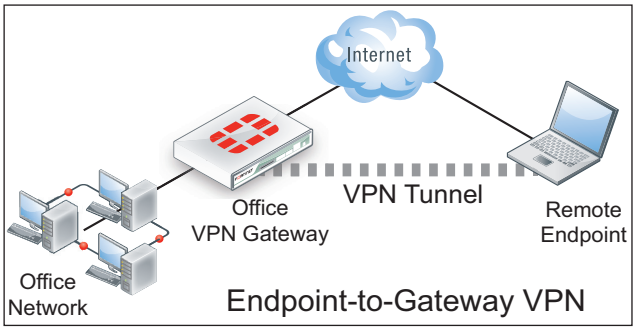
Fortinet VPN technology provides secure communications across the Internet between multiple networks and endpoints, through both IPsec and Secure Socket Layer (SSL) VPN technologies, leveraging FortiASIC hardware acceleration to provide high-performance communications and data privacy.



Benefits include enforcing complete FortiOS content inspection and multi-threat security for VPN communications, including antivirus, application control, IPS, web filtering, email filtering, sandboxing, Advanced Threat Protection (ATP), and Data Leak Prevention (DLP).

FortiOS IPsec and SSL VPNs support a full range of authentication options to identify users and to control access to resources. VPNs can authenticate individual users against the internal FortiOS user database or with external LDAP, RADIUS, or TACACS+ servers. Authentication can also use PKI or Windows directory service resources.

Both IPsec and SSL VPN tunnels can operate simultaneously on the same FortiGate unit. FortiOS VPNs are also compatible with FortiOS traffic optimization, traffic shaping, high availability, BYOD (device identification), and endpoint control.



Why use a VPN?

Virtual Private Network (VPN) technology enables users to transparently and securely cross the Internet between private networks. Any organization with off-site employees, more than one location connected to the Internet, or that communicates with other organizations over the Internet can benefit from employing a VPN solution because it ensures privacy of communication across the Internet.

Employees traveling or working from home can use endpoint-to-gateway VPNs to securely access the office network through the Internet. Employees in a branch office can use gateway-to-gateway VPNs to securely access main office resources. These VPNs ensure that unauthorized parties cannot intercept any of the protected information that is exchanged across the VPNs.

FortiOS IPsec VPN

FortiOS IPsec VPN supports all of the common industry standard IPsec features, including IKE v1 and v2, manual keys, static and dynamic gateway IP addresses, aggressive and main mode negotiation, pre-shared keys, X.509 security certificates, extended authentication (XAUTH), Diffie Hellman (DH) groups 1, 2, 5, and 14, dead peer detection, replay detection, perfect forward secrecy, and autokey keep alive.

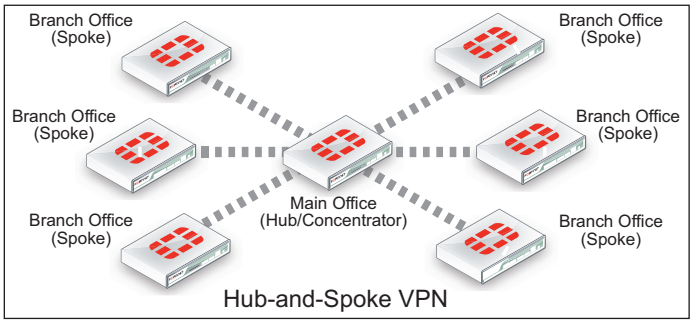
Fortinet IPsec VPNs employ industry standard features to ensure the best security and interoperability with industry standard VPN solutions provided by other vendors. FortiOS IPsec VPN encryption methods include DES, 3DES, AES128, AES192, and AES256. Authentication methods include MD5, SHA1, SHA256, SHA384, and SHA512.

FortiOS also supports policy-based and route-based IPsec VPNs. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that interface carries. Route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special IPsec VPN firewall policy that applies encryption (specified in the Phase 1 and Phase 2 VPN settings) to traffic accepted by the policy. To simplify the creation process, FortiOS includes an IPsec VPN configuration wizard that provides a quick and easy way to configure an IPsec VPN. The wizard includes templates for a number of common types of IPsec VPN, including options for both dialup and site-to-site VPNs.

Endpoint control ensures that network devices meet security requirements, otherwise they are not permitted access. FortiOS endpoint control is compatible with route-based VPNs if the VPN user is running FortiClient, which now supports iOS, Mac OS, Android OS, and Windows. This includes devices on private networks communicating over the IPsec VPN as well as devices that are operating as an IPsec VPN client using FortiClient to connect.

Other FortiOS IPsec VPN features include:

- **Hub-and-Spoke VPN:** Enables a head office to securely connect to all of its branch offices while enabling any branch office to communicate with any other branch office through the VPN concentrator. This provides the same connectivity as a full-mesh topology but uses a less complex configuration that provides central control of the VPN from the hub or concentrator.

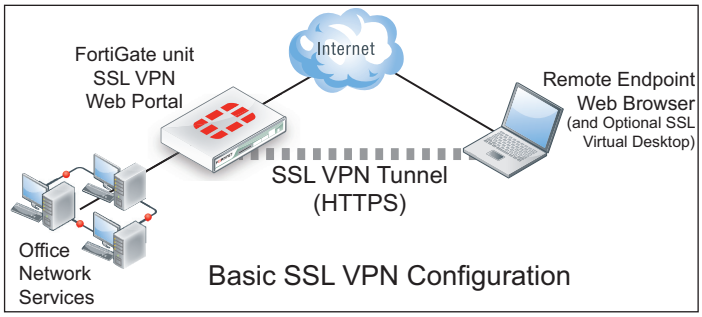


Hub-and-Spoke VPN

- **Hardware offloading:** Allows FortiASIC NP4 and NP6 network processors to provide accelerated processing for IPsec VPN traffic that would otherwise be processed by the FortiGate CPU. This improves IPsec tunnel performance as well as system performance by offloading processing from the CPU.
- **Dynamic routing over IPsec VPN tunnels:** Allows communication between complex multi-subnet networks over VPN so that complex private networks can be built on public (Internet) infrastructure. IPsec VPNs protect all traffic, including traffic routed by dynamic routing protocols—RIP, OSPF, BGP, and ISIS.
- **Redundant tunnels between VPN gateways:** Ensures that if the first tunnel goes down, the second tunnel is immediately available to carry traffic and seamlessly maintain service.
- **Compatibility with most third-party IPsec VPN gateway and client solutions:** FortiOS IPsec VPN is compatible with the VPN capabilities of Microsoft Windows (L2TP-IPsec), Cisco routers (GRE over IPsec), and iOS and Android mobile devices.
- **Automatic IPsec VPN configuration parameters for endpoints running FortiClient Endpoint Security:** Ensures that FortiClient users need only know their security credentials and the FortiGate VPN server IP address. FortiOS can also support auto-configuration of third-party clients that conform to the IKE Mode Config protocol.
- **IPsec VPN tunneling is performed at OSI Layer 3 (the Network layer) and below:** To enable remote access, encrypted network connectivity is established between a remote node and the internal network, thereby making the remoteness of the connection invisible to the IPsec VPN user. However, IPsec VPNs require potentially complex IPsec gateway and endpoint PC configurations.

FortiOS SSL VPN

SSL VPN gateway configurations are simpler than IPsec VPNs because they don't require specialized network configurations. SSL VPNs establish connectivity using SSL, which functions at OSI Levels 4 and 5 (the Transport and Session layers, respectively). Information is encapsulated at Levels 6 and 7 (the Presentation and Application layers). SSL VPNs communicate at the highest levels in the OSI model and are independent of the network architecture.



Using FortiASIC technology, FortiOS provides accelerated SSL encryption and decryption, which would otherwise be resource-intensive. The FortiGate SSL VPN service enforces complete content inspection and traffic optimization, as well as multi-threat protections including antivirus, intrusion prevention, and web filtering.

In most cases, additional configuration of SSL VPN endpoints is not required, since SSL is built into most web browsers (as HTTPS). Instead, users can connect to a FortiOS SSL VPN by opening any web browser, browsing to the FortiOS SSL VPN web portal, and logging in.

From the web portal, users can securely access resources on the protected network. The portal can also automatically install and invoke extended SSL VPN features, such as tunneling and virtual desktop protection, without user intervention or the need to configure SSL VPN settings on the endpoint.

SSL VPN Web Portal Mode

The SSL VPN web portal is a clientless method of providing secure remote access through a captive portal. The portal can be customized according to the user's authentication group and can include a custom look. Groups can also have pre-configured bookmarks to specific network resources, access to file servers, remote desktops, and SSH, telnet, file sharing, Citrix, and RDP applications. Users can also add their own personal bookmarks, which are not visible to other users. For resources that require authentication, bookmarks can include user credentials, thereby making the SSL VPN web portal a single sign-on (SSO) solution for remote users.

SSL VPN Tunnel Mode

SSL VPN tunnel mode is similar to IPsec VPN because it allows users to access protected network resources using their own applications instead of those provided in the web portal. Tunnel mode assigns a virtual IP address to the endpoint, and can be split so that only communication with the private network uses the tunnel. An Internet browsing configuration can send all of the SSL VPN user's Internet traffic through the tunnel. The SSL VPN user's traffic is then sent to the Internet from the FortiGate unit operating as the SSL VPN gateway and replies are sent back over the SSL VPN tunnel to the endpoint. FortiOS supports tunnel mode for Windows, Mac OS X, Linux, and selected mobile devices.

SSL VPN Port Forwarding

SSL VPN port forwarding listens on local ports on the user's computer, enabling a user to access applications, such as POP3 for email access, using the tunnel. When it receives data from a client application, the port forward module encrypts and sends the data to the FortiGate unit, which then forwards the traffic to the application server. The port forward module is implemented with a Java applet that downloads and runs on the user's computer.

Virtual Desktop

On a Microsoft Windows endpoint, SSL VPN sessions can be protected by the SSL VPN virtual desktop application that replaces the user's normal Windows desktop. Virtual desktop information is encrypted such that it becomes unavailable after the session ends, which is particularly useful if users are working with sensitive information.

The virtual desktop application 'control list' specifies the applications that users can access from the virtual desktop. The application control list and other virtual desktop options are configured on the FortiGate unit. Manual configuration of endpoint virtual desktops is not required.

Endpoint security checks

As part of the SSL VPN configuration, administrators can configure endpoint security checks to look at the endpoint's operating system version, its service pack level, and the existence of antivirus and/or firewall software.

Choosing between IPsec or SSL VPN

Even though IPsec and SSL VPNs use different technologies, both provide similar levels of security and are accelerated by FortiASIC technology. IPsec VPN operates at the network layer, so its configuration is generally more complex, requiring a greater understanding of potentially complex networking configurations, encryption, and authentication. However, IPsec VPN is the best solution for gateway-to-gateway VPNs connecting two or more private networks together over the Internet. Users can communicate transparently with resources on remote networks as long as they know the addresses of the remote network resources. Firewall policies can control the available networks and communication protocols. IPsec VPN is also the only solution for Hub-and-Spoke and redundant configurations where a single VPN must connect multiple networks through a single gateway or concentrator.

SSL VPN configurations are usually simpler than IPsec VPN configurations. All the complex networking is handled by the network infrastructure and the VPN configuration can focus on high-level communication requirements, access control, security profiles, and endpoint control. Some networks, such as those available in public spaces, may block IPsec protocols, thereby preventing IPsec endpoints from accessing their IPsec VPN gateways. An SSL VPN is the only workaround in this situation, since the HTTPS protocol used for SSL VPN is a standard Internet protocol required for many applications and is almost never blocked.

SSL VPN is the best solution for endpoint-to-gateway VPNs. Remote users can securely log into the SSL VPN web portal from any endpoint running a web browser that supports HTTPS, which could include PCs, tablets, and mobile devices. When a user logs into the SSL VPN web portal, their login credentials assign them appropriate security profiles. Their login credentials also determine the options and bookmarks that the web portal displays.

IPsec VPN can also be used for endpoint-to-gateway communication by installing IPsec VPN clients on the endpoints. This is a popular option used by many organizations, but SSL VPN is typically easier to configure and manage, and also provides better access control and security profile granularity.

SSL VPN is often used for communication between remote networks (similar to a gateway-to-gateway configuration). Users on one network could connect to a remote network by browsing to and logging into the remote network's SSL VPN portal. However, in most cases, an IPsec VPN gateway-to-gateway configuration makes it easier for users on remote networks to transparently connect to resources on other networks.

Conclusion

FortiOS supports both SSL and IPsec VPN technologies. Both technologies combine encryption and VPN gateway functions to create private communication channels over the Internet. They also define and deploy network access and firewall policies using a single management tool. Furthermore, both technologies support a simple client/user authentication process.

While you have the freedom to use either VPN technology, one may be more suitable to your situation than the other. IPsec VPNs are generally a good choice for site-to-site connections where appliance-based firewalls or routers are used to provide network protection, and where company-sanctioned client computers are issued to users. SSL VPNs are more suitable for roaming users who depend on a wide variety of thin-client computers to access enterprise applications and/or company resources from a remote location.